Draft FSA Security Training Content

Department of Education

Mandatory- The Computer Security Act of 1987 requires mandatory **annual** security awareness training by both Department employees and contractors working at the Department. Completion of the Department's For Your Eyes Only computer based training meets the annual training requirement.

Upcoming Specialized training is listed on the FSA Security Calendar.

Computer Based Training

The Department of Education has purchased sixty-four computer-based training (CBT) courses developed for the Department of Transportation's Virtual University (TVU) to supplement their IT Security Training Program. The EDVLC Course Curriculum and Mapping to Department of Education IT Security Positions is a guide that maps the different courses to the different security positions.

The Education Virtual Learning Center (ED VLC) IT Security Library User Guide, located at http://connected.ed.gov/doc_img/edvlc_it_sec_lib_userguide.doc, is a useful guide that explains how to:
Log in to the Education Virtual Learning Center (ED VLC) to take the IT Security Courses,
Change your password,
Select a course using the search catalog or course locator tool,
Select a course using the course locator tool by keyword or by category,
Add a course to your learning plan,
Start a course from your learning plan,
Navigate using the web player and web control panel, and
Exit a course properly to bookmark your last location.

Other

Commercial

SANS
The System Administration, Networking & Security (SANS) Institute
The SANS Institute was established in 1989 as a cooperative research and education organization. The SANS Institute enables more than 156,000 security professionals, auditors, system administrators, and network administrators to share the lessons they are

learning and find solutions to the challenges they face. At the heart of SANS are the many security practitioners in government agencies, corporations, and universities around the world who invest hundreds of hours each year in research and teaching to help the entire information security community.

SANS training provides a core set of educational courses designed to help master the practical steps necessary for defending systems and networks against the most dangerous threats - the ones being actively exploited. The courses were developed through the community consensus of hundreds of administrators, security managers, and information security professionals, and address both security fundamentals and the in-depth technical aspects of the most crucial areas of information security. SANS training can be taken in a classroom setting from SANS-certified instructors, or self-paced over the Internet. During 2001, more than 12,500 security, networking, and system administration professionals attended multi-day, in-depth training by the nation's top security practitioners and teachers.

SANS Institute instructor-led training programs are offered at several locations across the United States. More information about the various locations can be found at http://www.sans.org. SANS also provides On-Line Training, Instructor-Led On-Line Training, On-Line Training Group Licenses for groups of individuals, and On-site Training.

Training Library

The training library is a collection of media that FSA employees and contractors can borrow to learn more about security. If an employee/contractor is unable to access Connected, these materials provide an alternate way to access security training. The library is located at UCP cubicle # 101C3, or contact Robert.Clayton@ed.gov for more information. Materials are available for loan for a 2 week time period.

The following section describes the media that is currently available to borrow:

CDs

Federal Information System Security Awareness, Version 2.0, February 2002- Designed specifically for users of federal computer systems, this web based training product explains the importance of Information Systems Security. Topics include: threats and vulnerabilities, malicious code, user responsibilities, and new developments affecting Information Systems Security. Non-DOD government personnel should use this product as an alternative to DOD Information Assurance Awareness.

Information Age Technology, Version 2.1, July 2001- Intended for those who are not Information Technology Professionals but need to understand the terms and operations of the communications infrastructure, Information Age Technology V.2.1 brings the Information Age Technology presentation into the new millennium. This course

describes critical infrastructures and their relationship to the Internet. Using a transportation analogy to help students understand the behavior of networks, Information Age Technology V.2.1 provides an introduction to network hardware, such as routers, bridges, and gateways. The concepts of Uniform Resource Locator (URL), Domain Name System (DNS), Internet Protocol (IP) and 'browser' functions are also discussed. Finally, an interactive email exercise allows students to use several of the concepts presented.

Information Operations Fundamentals, Version 1.0, February 2001- IO Fundamentals provides an overview of IO in the joint context throughout the range of military operations. It addresses IO principles relating to both offensive and defensive IO and describes responsibilities for planning, coordinating, integrating, and deconflicting joint IO. IO Fundamentals is an update and expansion of INFOWAR Basics. The content is based upon DOD-centric security issues.

CyberProtect, Version 1.0, July 1999- CyberProtect is an interactive computer network defensive exercise with a video game look and feel. It is intended to familiarize players with information systems security terminology, concepts, and policy. Players learn about defensive security tools, which must be judiciously deployed on a simulated network. They then face a spectrum of security threats and must make practical decisions for allocating resources (in quarterly increments) using the elements of risk analysis and risk management. Play is divided into four sessions (simulating a fiscal year). After each session, players receive feedback on how well they are doing. At the end of the last session, players are given a report detailing their cumulative operational readiness rating. The report also details every attack by type, origin, and effectiveness of defensive tools. This cd requires loading on a PC or a server.

PKI- Public Key Infrastructure, Version 1.0, July 1999- This multimedia CD-ROM introduces PKI; what it is and the security services it provides. PKI user roles are discussed, including the functions of the Registration Authority (RA), Local Registration Authority (LRA) and the End User. User Registration is covered, as well as the generation and use of certificates and keys. The Resources section has points of contact for help with PKI, including useful web sites and PKI-related documents and templates. There is also a glossary of terms for reference. This cd requires loading on a PC or a server.

Windows NT Systems Security, Version 1.0, February 2001- Windows NT Security details the steps necessary to safeguard system resources in a stand-alone or networked Windows NT operating environment. It provides virtual hands-on exercises to reinforce instruction of key security features. The target audience for the product is system administrators, SSOs, and other personnel responsible for information systems administration. The user should have a basic hands-on understanding of computer systems and applications. The Resources section contains a library of Windows NT security documents to support and augment the content and exercises in the modules. There are also links to web sites related to Windows NT security.

Active Defense, Version 1, February 2003- This interactive training course is intended for executives in Information Assurance who are the key decision-makers in building a

security culture. The training serves as a strategic planning guide that introduces the issues and processes that must be understood in order to develop a strong commitment to protecting information resources. This course presents the goals of an information assurance program, explains why meeting these goals are essential to success, and distinguishes between the roles and responsibilities of all members of the organization. The course also explains how to identify and manage risks to information systems. Valuable checklists are provided at the end of each section.

Web Security, Version 1.3, June 2003- The Web Security web-based training (WBT) product is designed for DOD webmasters and others for use in the development and maintenance of websites for the DOD community. This interactive, multimedia training product covers legal issues, DOD policy and guidance, information protection, server side security and client side security. The audience for this product is System Administrators, Network Administrators, and users of the web, including web masters.

Database Security, Version 1.1, June 2003- This web-based course provides an overview of elements of database security. It is designed to provide training on Database Security for database administrators in training and general users. In addition, the course covers database concepts and terms, discusses privileges and roles used in controlling data access, and introduces profiles and tablespaces, which are used to limit system resources. These individual elements are discussed as they are applied together in the database environment. The last module pulls together the concepts learned throughout the course and applies them to various security methods used to secure the database.

Defense in Depth, Version 1.0, August 2001- Based on the Joint Vision 2020 concept of Information Superiority, and intended for military and civilian personnel responsible for the defense of DOD computers and computer networks, this web based training product explains the concept of 'Defense in Depth.' Using the multi-dimensional defenses of a mediaeval castle as a model, this presentation demonstrates the importance of a layered defense, which integrates the capabilities of People, Operations, and Technology. The user will learn how to defuse, detect, and react to a wide range of threats to networks, enclave boundaries, local computing environments, infrastructure support, and emerging technology.

OPSE 1301 - OPSEC Fundamentals CBT, February 2002- Describes the OPSEC (operation security) process using an OPSEC scenario.

Videos

Understanding Public Key Infrastructure (PKI), October 1998- This video introduces the concept of Public Key Infrastructure (PKI) and how it can be used to ensure the security and privacy of cyber-based transactions. Topics covered include examples of how PKI works, why it is necessary to protect the DII and NII, and how it ensures the confidentiality, integrity, non-repudiation, and authentication of electronic messages through digital signatures.

Information Assurance Compilation Series 1- This video covers a wide variety of information security topics, from an introductory portion to the importance of executives to how to safely destroy media.

Information Assurance Compilation Series 2- Topics include risks of cellular phones, identity theft, risks associated with fax machines, and information security standards.

Solar Sunrise, Dawn of a New Threat and Risky Business, June 2000- This video highlights the FBI/NIPC Solar Sunrise investigation involving computer hackers who gained access to Department of Defense computers during the 1998 Iraqi weapons inspection crisis. The second part of the video warns of economic espionage and the need to protect intellectual property from hackers and corporate competitors. The film centers on a real life case of economic espionage against a Colorado firm in 1994, which ultimately led to the Economic Espionage Act of 1996.

D*I*C*E 2003 Defensive Information to Counter Espionage- Ray Semko presents a dynamic assessment of the current threats to America. Focusing largely on terrorism and espionage, the D*I*C*E man stresses the need to protect our national security by applying the principles of OPSEC. He reaffirms the need to take security responsibilities personally, to stay aware and to report suspicious activities. This informative and inspirational presentation is a must see!

Certifications

Security certifications are another way to learn and apply knowledge of security topics. Certification programs involve intensive study of the topic culminating in a test to assess the knowledge. The following certifications are the most commonly recognized certifications for security.

CISSP-CISSP Certification was designed to recognize mastery of an international standard for information security and understanding of a Common Body of Knowledge (CBK). Certification can enhance a professional's career and provide added IS credibility.

CCSP- The CCSP (Cisco Certified Security Professional) certification provides network professionals with professional level recognition in designing and implementing Cisco secure networks. CCSP holders are actively involved in developing business solutions and designing and delivering multiple levels of security departments.

GSEC- General Security Certification from SANS Institute/GIAC is targeted at security professionals that want to fill the gaps in their understanding of technical information security; System, Security, and Network Administrators that want to understand the pragmatic applications of security; managers that want to understand information security beyond simple terminology and concepts; anyone new to information security with some background in information systems and networking. The GSEC tests the essential

knowledge and skills required of any individual with security responsibilities within an organization. GIAC also offers security certifications that are more highly specialized in topics such as firewalls or intrusion analyst.

- MCSE or MCSA- Microsoft has introduced two new certification specializations that identify IT professionals who demonstrate deep, role-based security skills on the Microsoft Windows® 2000 platform. These specializations provide a way for individuals to highlight their focus on security in the enterprise and demonstrate their ability to create a secure computing environment

Federal Guidance

NIST has issued several publications that relate to security training. One is NIST 800-50 Building an Information Technology Security Awareness and Training Program, which identifies four critical steps for training and awareness -- from assessing agency wide needs to post-implementation feedback and adjustment.